UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/277,335	03/26/1999	DEAN A. KLEIN	MPATENT.053A	3400

20995 7590 09/28/2005

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 09/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/277,335	**Applicant(s)** KLEIN, DEAN A.	
	Examiner Ponnoreay Pich	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 September 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-10,12-15,17 and 18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-10,12-15,17 and 18* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action. The examiner assumes that the applicant agrees with any well-known prior art statements and/or rejections made by the examiner in the previous office action(s) that were not argued.

This action is in response to applicant's amendments submitted on 9/20/2005. Claims 1, 5, 7, and 15 were amended. Claims 2, 11, and 16 were cancelled. Claims 1, 3-10, 12-15, and 17-18 are pending.

Response to Amendment

The examiner has considered applicant's amendments. Please see new rejections below.

The examiner notes that in the remarks submitted with the amendments on 9/20/2005, applicant's representative stated that "Based upon the interview and the Amendment of July 19, 2005, it is the Applicant's understanding that the ... amendments place all claims in condition for allowance." The examiner respectfully notes that this is not the case and the examiner had stated in the interview with applicant's representative that any amendments submitted by applicant **may** place the application closer to or in a condition of allowance, but whether or not it actually does depends on an updated search on the part of the examiner.

Prior to the amendments which were submitted on 7/19/2005 being entered into record, applicant's representative had held an interview with the examiner to determine if proposed amendments would overcome the prior art of record. The examiner stated that it would. However, after the amendments were entered on 7/19/2005 and on further review by the examiner, the examiner came to the conclusion that the amendments would not overcome the prior art of record. Rather than issuing a Final rejection for set of claims submitted on 7/19/2005, the examiner contacted applicant's representative on 8/31/2005 and gave applicant's representative an opportunity to submit further amendments which would overcome the prior art of record. The examiner notes that the arguments submitted with the amendments on 7/19/2005 stated that a similar amendment was used to get related US application 09/277,482 allowed. The examiner reviewed the prosecution history for application 09/277,482 and notes that the limitation that made that application allowable was more limiting than what applicant's representative amended onto the set of claims for the current application on 7/19/2005.

Applicant's representative submitted informal amendments to the examiner on 9/1/2005 and asked if the amendments were enough to get the case allowed. The informal amendments had a note that they not be entered into record. The examiner asked the opinion of a primary in his art unit about the proposed amendments getting the case allowable, as applicant's representative had indicated that he was willing to work with the office to amend the claims as necessary to get the application allowed. The primary stated that the proposed amendments alone probably would not make the case allowable. However, incorporating the proposed amendments (informal amendments submitted on 9/1/2005) along with the limitations from claims 2 and 16 into the independent claims as well as fixing any 112, second paragraph problems missed would get the case closer to allowance than just the proposed amendments alone. The examiner relayed this information to applicant's representative in the interview held on 9/12/2005 and the examiner thought applicant's representative understood that the proposed informal amendments sent to the examiner on 9/1/2005 along with the limitations in claims 2 and 16 if incorporated into the independent claims of the current application would place the application in a condition for possible allowance over art.

The examiner notes that the amendments applicant's representative submitted on 9/20/2005 instead has the amendments which were submitted on 7/19/2005 and the limitations from claims 2 and 16 incorporated into the independent claims. The informal amendments communicated to the examiner on 9/1/2005 are not the same as the amendments submitted on 7/19/2005. The current set of amendments submitted on 9/20/2005 are not what the examiner was expecting to have been submitted based on the interview the examiner held with applicant's representative on 9/12/2005. The examiner's rejections below are based on the amendments which were submitted on 9/20/2005.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1, 3-10, 12-15, and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olarig et al (US 6,032,257) in view of van Rumpt et al (US 5,513,262), herein referred to as Rumpt1, and van Rumpt et al (US 5,231,662), herein referred to as Rumpt2, further in view of Easter et al (US 5,563,950) and further in view of Tsukamoto et al (US 5,796,828).

Claim 1:

Olarig discloses the limitations of:

1. Storing an identification code in a non-erasable memory during manufacture of the personal computer, wherein said identification code is defined at least in part by information associated with components of said personal computer (col 5, lines 25-65; col 6, lines 24-27; col 8, lines 10-15; and Fig 3, item 140).
2. Retrieving the identification code from the memory in said personal computer (col 9, lines 1-10).
3. Generating a cryptographic key derived at least in part from said identification code (col 9, lines 25-35).

Olarig does not explicitly disclose:

1. Receiving user input.
2. Generating a cryptographic key derived at least in part from the received user input.
3. Retrieving a checksum from a configuration register in a bus-to-bus bridge in the personal computer.

4. Verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated key.
5. Encrypting and decrypting data, for storage on and retrieval from one of said data storage media using said cryptographic key, wherein the data is transmitted by the processor and is encrypted in the personal computer by the encryption hardware.
6. Retrieving information from a memory location.
7. Disabling encryption of data routed to one of said data storage media in response to said retrieved information.

However, Rumpt2 discloses:

1. Receiving user input (abstract; Fig 1; and col 3, liens 17-59).
2. Generating a cryptographic key derived at least in part from the received user input (Fig 1 and col 3, lines 17-59).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill to combine the above teachings of Rumpt2 with Olarig. One of ordinary skill would have been motivated to do so because Rumpt2's teachings would allow for an owner of a personal computer as disclosed by Olarig to encrypt the data storage unit in the personal computer such that only the owner can decrypt the content of the data storage unit. The key is partially derived from the user input, so only the user would know what the key is. This would deter theft of the personal computer or at the very least make it harder for a thief to gain access to the data on the computer should it be stolen. Note, Olarig's teachings are directed towards theft protection for computers and computer related hardware (col 2, lines 5-6).

Further, Rumpt1 discloses a configuration register in a bus-to-bus bridge in the personal computer (Fig 1 and Fig 2). Note that data encryption unit 2 is the bus-to-bus bridge as it bridges AT bus 1 and IDE bus 3. Easter discloses calculating a hash value for a cryptographic key and storing the hash value (col 5, lines 32-35 and col 6, lines 23-25). Note that a checksum is a hash value. Easter also discloses verifying a generated cryptographic key by calculating the hash value of the key and then comparing the calculated hash value of the key with the stored hash value (col 6, lines 23-24 and 48-50). Note that the place the first hash/checksum was stored reads on a configuration register. To compare the two hashes/checksums, the first hash/checksum value must be obtained from the configuration register. The combination of these two teachings by Rumpt1 and Easter read on the limitations of retrieving a checksum from a configuration register in a bus-to-bus bridge in the personal computer and verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated key.

Rumpt1 further discloses the limitation of encrypting and decrypting data, for storage on and retrieval from one of said data storage media using said cryptographic key, wherein the data is transmitted by the processor and is encrypted in the personal computer by the encryption hardware (col 3, lines 10-20 and col 2, lines 40-45).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to combine Rumpt1 and Easter's teachings within the combination invention of Olarig and Rumpt2. One of ordinary skill would have been motivated to incorporate Rumpt1's teachings because Rumpt1's teachings would enable the combination invention of Olarig and Rumpt2 to encipher or decipher data in a simple and fast manner (Rumpt1: col 1, lines 33-37). One of ordinary skill would be motivated to incorporate Easter's teachings because Easter discloses that it is desirable to verify that a cryptographic key is good before it is used (col 6, lines 28-34). This would prevent data from being encrypted with a faulty key, which might result in poorly secured data or data which cannot be decrypted.

As per the limitations of retrieving information from a memory location and disabling encryption of data routed to one of said data storage media in response to retrieved information, they are met by Tsukamoto (col 4, lines 4-18; col 5, lines 5-10; and col 9, lines 23-37). At the time applicant's invention was made it would have been obvious to one of ordinary skill in the art to incorporate Tsukamoto's teachings into the combination invention of Olarig, Rumpt1, Rumpt2, and Easter according to what is recited in claim 1. One of ordinary skill would have been motivated to do so as Tsukamoto's teachings would allow the owner of the personal computer to selectively choose which data to encrypt and which to keep unencrypted. For instance, one might want to keep the owner's contact information unencrypted in case a personal computer, i.e. laptop, is accidentally lost; the owner would want whoever finds it to be able to return the laptop to the owner if the person who found the laptop is an honest person.

Claim 3:

Olarig further discloses said retrieving is performed without intervention by a host processor (col 9, lines 4-10).

Claim 4:

Olarig further discloses verifying said key, wherein said verifying occurs without intervention of said host processor (col 9, lines 15-25).

Claim 13:

The limitation of encryption data for storage is performed on an encrypting device that is positioned in a data path between a central processing unit and the data storage medium is obvious to the combination invention of Olarig, Rumpt1, Rumpt2, Easter, and Tsukamoto as Rumpt1 discloses it (Fig 1; col 2, lines 5-20).

Claim 14:

The limitation of wherein all data is transmitted to the data storage media is encrypted is obvious to the combination invention of Olarig, Rumpt1, Rumpt2, Easter, and Tsukamoto as Rumpt1 discloses it (col 3, lines 5-20).

Claim 5:

Olarig discloses the limitations of:

1. Storing a hardware identifier in a non-erasable memory integrated circuit at the time of manufacturing of the computer, wherein the hardware identifier is defined at least in part by information associated with components of said computer (col 5, lines 25-65; col 6, lines 24-27; col 8, lines 10-15; and Fig 3, item 140).

2. Installing said memory integrated circuit into said computer (col 6, lines 22-27 and Figures 1 and 3).
3. Providing a data path to data storage media (Figures 1 and 3).
4. Connecting said memory integrated circuit to a logic circuit (Figures 1 and 3).
5. Generating a cryptographic key derived at least in part from a hardware identifier (col 9, lines 25-35)

Olarig does not disclose the limitations of:

1. Providing a configuration in a bus-to-bus bridge for storing a checksum.
2. Coupling a logic circuit comprising an encryption engine to said data path.
3. Wherein the hardware identifier and user input is used by the encrypting engine for encrypting data that is transmitted to the data storage media and for decrypting data that is retrieved from the data storage media, wherein the encryption engine verifies the generated cryptographic key using the checksum, and wherein the encryption engine is configured to disable encryption of data routed to the data storage media in response to information retrieved from a storage location.

However, Rumpt1 discloses providing a configuration in a bus-to-bus bridge (Fig 1, item 2 and Fig 2). Rumpt1 discloses coupling a logic circuit comprising an encryption engine to a data path (Fig 1).

Further, as discussed in claim 1, Easter discloses calculating a hash value fur a cryptographic key and storing the hash value (col 5, lines 32-35 and col 6, lines 23-25). Easter also discloses verifying a generated cryptographic key by calculating the hash value of the key and then comparing the calculated hash value of the key with the stored hash value (col 6, lines 23-34 and 48-50). The examiner asserts that the structure in which the hash value is stored is a configuration.

Further, Rumpt2 discloses receiving user input (abstract; Fig 1; and col 3, lines 17-59) and generating a cryptographic key derived at least in part from the received user input (Fig 1 and col 3, lines 17-59).

Further, Tsukamoto discloses disabling encryption of data routed to the data storage media in response to information retrieved from a storage location (col 4, lines 4-18; col 5, lines 5-10; and col 9, lines 23-37).

In light of the above teachings by Rumpt1, Rumpt2, Easter, and Tsukamoto, it would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify Olarig's invention according to the limitations recited in claim 5. One of ordinary skill would have been motivated to incorporate Rumpt1, Rumpt2, Easter, and Tsukamoto's teachings with Olarig for the same reasons given in claim 1.

Claim 6:

The limitation of said act of connecting comprises routing a serial data bus from said memory integrated circuit to said logic circuit is obvious to the combination invention of Olarig, Rumpt1, Rumpt2, Easter, and Tsukamoto as Rumpt1 discloses it (col 2, lines 1-25).

Claim 7:

The limitations recited in claim 7 though worded slightly differently are substantially similar to what is recited in claim 1. As such, claim 7 is rejected for the same reasons as claim 1.

Claim 8:

The limitation of wherein said information is permanently associated with said hosting computing logic is obvious to the combination invention of Olarig, Rumpt1, Rumpt2, Easter, and Tsukamoto as it is disclosed by Olarig (col 5, line 67-col 6, line 3).

Claim 9:

The limitation of said information comprises a multi-bit identification code is obvious to the combination invention of Olarig, Rumpt1, Rumpt2, Easter, and Tsukamoto as Rumpt2 discloses a multi-bit identification code (col 3, lines 15-65).

Claim 10:

The limitation of the act of deriving an encryption key is at least in part from said identification code is obvious to the combination invention of Olarig, Rumpt1, Rumpt2, Easter, and Tsukamoto as Rumpt2 discloses deriving an encryption key at least in part from an identification code (col 6, lines 10-25).

Claim 12:

The limitation of defining said encryption process at least in part from user input to said computer system is obvious to the combination invention of Olarig, Rumpt1, Rumpt2, Easter, and Tsukamoto as Rumpt2 discloses it (col 3, lines 15-45).

Claim 15:

The limitations recited in claim 15 are substantially similar to what is recited in claim 5. As such the rejection for claim 1 applies to claim 15. One difference is that in claim 15, line 18, there is an additional limitation not found in claim 1: "wherein the encryption hardware is part of the bus-to-bus bridge circuit". However this limitation is obvious to the combination invention of Olarig, Rumpt1, Rumpt2, Easter, and Tsukamoto as Rumpt 1 clearly shows the encryption hardware is part of the bus-to-bus bridge circuit (Fig 1 and 2). See in Figure 1, data encryption unit 2 bridges two buses and in Fig 2, the encryption unit contains encryption hardware.

Claims 17 and 18:

As per claims 17 and 18, they recite limitations substantially similar to what is found in claims 3 and 4 respectively and are rejected for the same reasons.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100